Experimental results on smartcards' IC EM radiation

N. Mendo*, R. Nuevo, D. Hernández

IT Labs, Applus Laboratories, C\ Ronda de la Font del Carme S/N, 08193, Bellaterra, Barcelona, Spain

* natalia.mendo@applus.com

Electromagnetic (EM) radiation is a powerful source of information that can be used to exploit confidential information leaking from an IC. In hardware components executing operations, electromagnetic radiation comes from currents flowing through bus and address lines, and also from logic gates and transistors switching on and off during execution. As these emanations are related to the operations conducted on the IC, this relationship can be used to recover sensitive information.

Since the milestone paper of P. Kocher presenting power analyses, many works have focused on developing power attacks mainly on crypto modules. Differential and correlation analyses[1,2] are used to retrieve the secret key of crypto-algorithms from the EM radiated by the IC by conducting statistical analyses. The efficiency of these attacks is directly related to the quality of the signal acquired. I.e., the Signal-to-Noise-Ratio, the position of the antenna, or the polarization of EM radiation play an important role on the final attack results. Despite these considerations, few studies have been published on the experimental realizations of such attacks when considering the specifications of the different measurement tools such as antennas, oscilloscopes, or the wiring.

In this work we investigate on the EM radiation of ICs from smartcards analyzing the exploitable leakage obtained from different antennas and filtering techniques. The work is conducted on an ARM smart card device with AES-128 algorithm implemented by software. Differential Electromagnetic Analysis on AES is used to characterize the leakage of chip's radiation. Hence, experimental results will reveal practical information of the device.

[1] Kocher, P.C., Jaffe, J., Jun B.: Differential power analysis. In: Lecture Notes in Computer Science, vol. 1666, pp. 388–397 – Proceedings of CRYPTO'99 (1999)

[2] Brier, E., Clavier, C., Olivier, F.: Correlation power analysis with a leakage model. In: Lecture Notes in Computer Science, vol. 3156, pp. 16–29 – Proceedings of CHES 2004 (2004)